The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
11/14/2011

SUBJECT:
Multiple Vulnerabilities in Adobe Flash Player Could Allow For Remote Code Execution (APSB11-28)

OVERVIEW:
Multiple vulnerabilities have been discovered in Adobe Flash Player that could allow attackers to take complete control of affected systems. Adobe Flash Player is a widely distributed multimedia and application player used to enhance the user experience when visiting web pages or reading email messages. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

SYSTEMS AFFECTED:
- Adobe Flash Player 11.0.1.152 and earlier versions for Windows, Macintosh, Linux and Solaris
- Adobe Flash Player for Android 11.0.1.153 and earlier versions
- Adobe AIR 3.0 and earlier versions for Windows, Macintosh, and Android

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:
Adobe Flash Player is prone to multiple vulnerabilities that could allow for remote code execution. Details of these vulnerabilities are as follows:
- Eight memory corruption vulnerabilities which could allow for remote code execution
- A heap corruption vulnerability which could lead to code execution
- A buffer overflow vulnerability which could lead to code execution
- A stack overflow vulnerability which could lead to code execution
- A cross-domain policy bypass vulnerability

These vulnerabilities may be exploited if a user opens a specially crafted Adobe Flash file. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

RECOMMENDATIONS:
We recommend the following actions be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Do not open email attachments or click on URLs from unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails, IM (Instant Messages) or attachments especially from un-trusted sources.
- Consider implementing file extension whitelists for allowed e-mail attachments.

REFERENCES:

Adobe:
http://www.adobe.com/support/security/bulletins/apsb11-28.html

Security Focus:
http://www.securityfocus.com/bid/50618
http://www.securityfocus.com/bid/50619
http://www.securityfocus.com/bid/50620
http://www.securityfocus.com/bid/50621
http://www.securityfocus.com/bid/50622
http://www.securityfocus.com/bid/50623
http://www.securityfocus.com/bid/50624
http://www.securityfocus.com/bid/50625
http://www.securityfocus.com/bid/50626
http://www.securityfocus.com/bid/50627
http://www.securityfocus.com/bid/50628
http://www.securityfocus.com/bid/50629

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2445
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2450
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2451
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2452
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2453
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2454
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2455
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2456
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2457
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2458
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2459
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2460